UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/041,071	12/28/2001	Andrew F. Glew	42390.P13769	5239

59796 7590 12/08/2008

INTEL CORPORATION
c/o INTELLEVATE, LLC
P.O. BOX 52050
MINNEAPOLIS, MN 55402

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	PAPER NUMBER
2437	
MAIL DATE	DELIVERY MODE
12/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/041,071	GLEW ET AL.	
	Examiner	Art Unit	
	Tamara Teslovich	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 August 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-4 and 6-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-4 and 6-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office action is in response to Applicant's Remarks filed August 18, 2008.

Claims 1, 5 and 14-34 remain cancelled.

Claims 2-4 and 6-13 are pending and herein considered.

Response to Arguments

Applicant's arguments filed August 18, 2008 have been fully considered but they are not persuasive.

In response to Applicant's first set of arguments appearing on page 2 of the remarks concerning England's alleged failure to describe "an instruction to launch a code module to establish a trusted system environment" as claimed in claim 3, the Examiner respectfully disagrees. The Examiner draws attention first and foremost to column 3, lines 36-44 wherein England teaches a "new class of secure operation called curtained execution, because it can be curtained off and hidden from the normal operations of the system. The Examiner has equated England's "curtained execution" with Applicant's "trusted system environment" insofar as it serves to securely execute particular code modules in an environment where access to memories, processors and any other communication to the system are limited based on their trustworthiness in order to provide a trusted system environment that may be trusted. The Examiner maintains that England's operation of these "trusted code modules" from secure memory without interruption by any other processes teaches Applicant's "trusted system environment" while England's "CCALL instruction" to launch a module to verify that the

necessary privileges and protections are in order to establish the trusted system teaches Applicant's "instruction to launch a code module to establish a trusted system environment" (col.9 line 52 thru col.10 line 65).

In response to Applicant's next set of arguments appearing on page 2 of the remarks concerning England's alleged failure to describe "verifying, by the processor in response to receiving an instruction, that the environment of the processor is appropriate to launch the code module" as claimed in claim 3, the Examiner respectfully disagrees. The Examiner would first like to draw attention to column 6, lines 53-45 wherein England discloses the loading of code and data "under the proper conditions." These conditions, or "appropriateness" as Applicant prefers to call them, are further elaborated on in column 9 lines 60 thru 67 as well as the entirety of column 10. England discloses in these portion, "logic 356" that may be used to determine whether or not to execute a curtained code by comparing the rights of that particular piece of code, whether or not the processor is already busy executing some other curtained code, and whether the code exists within secure memory. These are just a few of the checks that England's system does before verifying in response to receiving a CCALL instruction, that the environment of the processor, memory, and general status of the computer, is appropriate to launch the code module.

In response to Applicant's third set of arguments appearing on page 2 of the remarks concerning England's alleged failure to describe "updating, by the processor in response to verifying that the environment of the processor is appropriate, event processing to support launching the code module" as claimed in claim 3, the Examiner

respectfully disagrees. The Examiner would first like to draw attention to column 8 lines 65-67 and column 9 lines 1-19 wherein England discloses the verification procedure discussed above, as well as the way in which certain opcodes are restricted to executing only when the CPU is in a trusted system environment executing curtained code. England goes on in column 10, lines 25-65 the way in which the "control unit 350 must ensure atomicity in executing the curtained code" in order that "once started, the code must perform its entire operation without interruption from any point outside the secure curtained-memory regions." England takes this one step further, but "prevent[ing] interrupt[s] from subverting curtained code" by issuing a "privileged instructions that [cause] a microprocessor to switch off all interrupts until a companion instruction switches them back on." By updating the processor's event processing in this way, the curtained code module may be launched and securely executed in response to verifying that the code module is in fact appropriate and that the system and its memories and processors are ready and able to run it securely.

Regarding Applicant's next set of arguments appearing at the top of page 3 of the remarks and consisting of a general listing of the remaining limitation of claim 3, Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. A simple listing of claim limitations followed by a general statement that the reference "does not describe any of these limitations" is insufficient insofar as it

amounts to a general statement of patentability without acknowledging those sections specifically sited by the Examiner in her rejection of those limitations.

It is based upon the arguments presented above in view of the reference in its entirety that the Examiner maintains her 35 USC 102 rejection of claims 2-4 and 6-13.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 2-4 and 6-13 remain rejected under 35 U.S.C. 102(e) as being anticipated by US Patent No. 6,651,171 B1 by England et al.

Regarding **claim 2**, England discloses transferring a number of bytes specified by an operand from a memory (col.7 lines 35-56).

Regarding **claim 3**, England discloses a method comprising

receiving, by a processor, an instruction to launch a code module to establish a trusted system environment (col.8 lines 42-44; col.9 line 52 thru col.10 line 65);

verifying, by the processor in response to receiving the instruction, that the environment of the processor is appropriate to launch the code module (col.6 lines 53-54; col.8 lines; col.9 line 60 thru column 10 line 65; col.15 lines 40-44);

updating, by the processor in response to verifying that the environment of the processor is appropriate, event processing to support launching the code module (col.8 lines 34-48 and 65-67; column 9 lines 1-19; col.10 lines 25-65);

locking, by the processor in response to updating event processing, a processor bus coupling the processor to other processors (col.9 lines 15-19; col.10 lines 51-55, 61-65; col.11 lines 36-39);

configuring, by the processor in response to locking the processor bus, a cache memory of a processor to operate in a private ("curtained") mode in which requests within the memory range of the cache are satisfied by the cache and cache lines are not replaced or invalidated in response to snoop requests on the processor bus (col.3 lines 35-43; col.7 lines 43-48; col.10 line 55-59),

transferring, by the processor in response to configuring the cache memory to operate in the private mode, the code module to the cache memory of the processor (col.7 lines 43-48);

determining, by the processor in response to transferring the code module to the cache memory, that the code module stored in the cache memory is authentic col.7 lines 48-52; col.8 lines 11-14) and

executing the code module from the cache memory in response to determining that the code module is authentic (col.8 lines 2-4).

Regarding **claim 4**, England discloses invalidating the cache memory prior to storing the code module in the cache memory (col.6 lines 6-67).

Regarding **claim 6**, England discloses determining whether the code is authentic based upon a digital signature of the code module (col.13 lines 27-40).

Regarding **claim 7**, England discloses obtaining a first value from the code module stored in the cache memory and computing a second value from the code module (col.13 lines 15-26); and determining that the code module is authentic in response to the first value and the second value having a predetermined relationship (col.7 lines 1-34, 57-67; col.13 lines 15-26, 61-67).

Regarding **claim 8**, England discloses retrieving a key (col.13 lines 15-26), decrypting a digital signature of the code module with the key to obtain a first value and hashing the code module to obtain a second value (col.13 lines 15-26); and executing the code module in response to the first value and the second value having a predetermined relationship (col.13 lines 15-40, 61-67).

Regarding **claim 9**, England discloses wherein decrypting comprises using the key to RSA-decrypt the digital signature, and hashing comprises apply a SHA-I hash to the code module to obtain the second value (col.13 line 8 thru col.15 line 50).

Regarding **claim 10**, England discloses retrieving the key from a processor used to execute the code module (col.15 lines 19-52; ol.11 lines 27-39).

Regarding **claim 11**, England discloses retrieving the key from a chipset (col.15 lines 19-52; col.11 lines 27-39).

Regarding **claim 12**, England discloses retrieving the key from a token (col.7 lines 57-67).

Regarding **claim 13**, England discloses receiving the code module from a machine readable medium (col.6 lines 35-46).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571)272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tamara Teslovich/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437